UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/631,989	07/31/2003	Bjorn Markus Jakobsson	EMC-06-463	2203

80167 7590 08/04/2009

Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560

EXAMINER	
TESLOVICH, TAMARA	
ART UNIT	PAPER NUMBER
2437	
MAIL DATE	DELIVERY MODE
08/04/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/631,989	JAKOBSSON ET AL.	
	Examiner	Art Unit	
	Tamara Teslovich	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 April 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

A request for continued examination under 37 CFR 1.114 was filed in this application after appeal to the Board of Patent Appeals and Interferences, but prior to a decision on the appeal. Since this application is eligible for continued examination under 37 CFR 1.114 and the fee set forth in 37 CFR 1.17(e) has been timely paid, the appeal has been withdrawn pursuant to 37 CFR 1.114 and prosecution in this application has been reopened pursuant to 37 CFR 1.114. Applicant's submission filed on April 13, 2009 has been entered.

Claims 1-30 are pending and herein considered.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-30 are rejected under 35 U.S.C. 102(b) as being anticipated by United States Patent No. 2002/0094088 to Takumi Okaue

As per **claim 1**, Okaue teaches a method for partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality from a delegating device to at least one recipient device,

the cryptographic functionality being characterized as a graph comprising a plurality of nodes (par 15 "hierarchy key tree structure" ; par 16 “key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of the key tree structure comprising a plurality of devices”) comprising the steps of:

associating a given set of the nodes with a corresponding one of the plurality of distinct portions of the cryptographic functionality (par 22 “these leaf-keys are respectively provided in correspondence with own leaves among a hierarchy key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of the key tree structure comprising a plurality of data processing apparatuses as own leaves”; par 92 “each of individual leaves of the hierarchical tree structure corresponds to respective contents data reproducing device”); and

transmitting from the delegating device to the recipient device information representative of one or more of the nodes (pars 82, 84, 90-91, par 96 “provider delivers the ciphered common contents data or such a contents data key commonly usable by individual devices to those devices"),

the recipient device being configured based on the transmitted information for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality (pars 82, 84, 90-91);

wherein the nodes of the graph are arranged in a plurality of levels with one or more nodes at each level wherein the nodes correspond to respective seeds (par 22

“these leaf-keys are respectively provided in correspondence with own leaves among a hierarchy key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of the key tree structure comprising a plurality of data processing apparatuses as own leaves”);

wherein a first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level (pars 23-24, 97-105, 114-117);

the transmitted information including the first seed but not the second seed (par 96 “provider delivers the ciphered common contents data or such a contents data key commonly usable by individual devices to those devices").

As per **claim 2**, Okaue teaches wherein at least one of the nodes of the graph corresponds to a seed the possession of which permits execution of a corresponding one of the distinct portions of the cryptographic functionality (par 82).

As per **claim 3**, Okaue teaches wherein the transmitting step further comprises transmitting from the delegating device to the recipient device information representative of at least two of the nodes (par 96 “provider delivers the ciphered common contents data or such a contents data key commonly usable by individual devices to those devices"; par 97).

As per **claim 4**, Okaue teaches wherein the transmitting step further comprises transmitting from the delegating device to the recipient device information representative of at least one parent node of the graph (pars 98, 123,131-134).

As per **claim 5**, Okaue teaches wherein the transmitting step further comprises transmitting from the delegating device to the recipient device information representative of at least one child node of a parent node of the graph (pars 98, 123,131-134).

As per **claim 6**, Okaue teaches wherein the graph comprises at least first and second root nodes (pars 132, 134).

As per **claim 7**, Okaue teaches wherein the graph comprises a tree having at least first and second subtrees associated with respective first and second ones of the plurality of distinct portions of the cryptographic functionality (par 105).

As per **claim 8**, Okaue teaches wherein the graph comprises a chain (pars 132-135).

As per **claim 9**, Okaue teaches wherein the graph comprises L levels of nodes, an Lth one of the levels comprising a parent node v.sub.L,1, and a first one of these levels comprising a set of seeds v.sub.1,1, v.sub.1,2, . . . v.sub.1,n, where n is the total

number of seeds, each of the seeds being derivable from the parent node (pars 23-24, 97-105, 114-117).

As per **claim 10**, Okaue teaches wherein an ith node of a kth one of the levels is computed as f.sub.k(i, v.sub.k+1), where f.sub.k is a one-way function (pars 23-24, 97-105, 114-117).

As per **claim 11**, Okaue teaches wherein the nodes of one or more of the levels are arranged in the form of tuples of designated numbers of nodes (pars 23-24, 94, 97-105, 114-117).

As per **claim 12**, Okaue teaches wherein the ith node of a jth tuple of the kth level is computed as f.sub.k(j, i, v.sub.k+1,j) (pars 23-24, 94, 97-105, 114-117).

As per **claim 13**, Okaue teaches wherein the cryptographic functionality comprises a cryptographic functionality provided by a hardware-based authentication token (pars 30-32, 83, 85, 87-89).

As per **claim 14**, Okaue teaches wherein the cryptographic functionality comprises an ability to verify at least one of an authentication code and a distress code generated by a hardware-based authentication token (pars 30-32, 83, 85, 87-89).

As per **claim 15**, Okaue teaches wherein the authentication token is configured to store at least two seeds, and the cryptographic functionality comprises a verification operation performed collaboratively by at least first and second servers each storing one of the seeds (pars 30-32, 83, 85, 87-89).

As per **claim 16**, Okaue teaches wherein the cryptographic functionality comprises an ability to generate at least one of an authentication code and a distress code utilizing a hardware-based authentication token (pars 30-32, 83, 85, 87-89).

As per **claim 17**, Okaue teaches wherein the cryptographic functionality comprises at least one of an ability to verify a signature and an ability to generate a signature (pars 82, 119).

As per **claim 18**, Okaue teaches wherein the cryptographic functionality comprises an ability to generate one or more values of a one-way chain (pars 132-135).

As per **claim 19**, Okaue teaches wherein the cryptographic functionality comprises an ability to perform symmetric cryptographic operations (pars 15, 82-85, 10, 87).

As per **claim 20**, Okaue teaches wherein the cryptographic functionality comprises an ability to perform asymmetric cryptographic operations (pars 15, 82-85, 10, 87) .

As per **claim 21**, Okaue teaches wherein the cryptographic functionality comprises an ability to derive one or more cryptographic keys (pars 15, 82-85, 10, 87).

As per **claim 22**, Okaue teaches wherein the cryptographic functionality comprises an ability to compute one or more seeds (pars 15, 82-85, 10, 87).

As per **claim 23**, Okaue teaches wherein at least one of the seeds corresponds to at least one of the nodes of the graph (pars 15, 82-85, 10, 87).

As per **claim 24**, Okaue teaches wherein the cryptographic functionality is partitioned in accordance with a subscription model which requires compliance with at least one specified criterion for transmission from the delegating device to the recipient device of the information representative of one or more of the nodes (pars 2-3, 7, 13, 96).

As per **claim 25**, Okaue teaches wherein compliance with the specified criterion is satisfied upon receipt of a designated payment (par 96).

As per **claim 26**, Okaue teaches wherein the recipient device and the delegating device collaborate to perform at least one of a cryptographic verification function and a cryptographic generation function (par 82).

As per **claim 27**, Okaue teaches wherein the recipient device includes only a limited computational ability associated with performance of the cryptographic function (pars 83-85).

As per **claim 28**, Okaue teaches an apparatus comprising:

a processing device comprising a processor coupled to a memory (pars 82-89)

the processing device being utilized in conjunction with partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality from the processing device, configured as a delegating device, to at least one recipient device, the cryptographic functionality being characterized as a graph comprising a plurality of nodes (par 15 "hierarchy key tree structure" ; par 16 "key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of the key tree structure comprising a plurality of devices");

the processing device being configured to associate a given set of the nodes with a corresponding one of the plurality of distinct portions of the cryptographic functionality (par 22 "these leaf-keys are respectively provided in correspondence with own leaves

among a hierarchy key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of the key tree structure comprising a plurality of data processing apparatuses as own leaves"; par 92 "each of individual leaves of the hierarchical tree structure corresponds to respective contents data reproducing device"), and to transmit to the recipient device information representative of one or more of the nodes (pars 82, 84, 90-91, par 96 "provider delivers the ciphered common contents data or such a contents data key commonly usable by individual devices to those devices");

the recipient device being configured based on the transmitted information for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality (pars 82, 84, 90-91);

wherein the nodes of the graph are arranged in a plurality of levels with one or more nodes at each level and wherein the nodes correspond to respective seeds (par 22 "these leaf-keys are respectively provided in correspondence with own leaves among a hierarchy key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of the key tree structure comprising a plurality of data processing apparatuses as own leaves");

wherein a first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level (pars 23-24, 97-105, 114-117);

the transmitted information including the first seed but not the second seed (par 96 "provider delivers the ciphered common contents data or such a contents data key commonly usable by individual devices to those devices").

As per **claim 29**, Okaue teaches an apparatus comprising: a processing device comprising:

a processor coupled to a memory (pars 82-89)

the processing device being utilized in conjunction with partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality to the processing device, configured as a recipient device, from at least one delegating device, the cryptographic functionality being characterized as a graph comprising a plurality of nodes (par 15 "hierarchy key tree structure" ; par 16 "key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of the key tree structure comprising a plurality of devices");

a given set of the nodes being associated with a corresponding one of the plurality of distinct portions of the cryptographic functionality (par 22 "these leaf-keys are respectively provided in correspondence with own leaves among a hierarchy key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of the key tree structure comprising a plurality of data processing apparatuses as own leaves"; par 92 "each of

individual leaves of the hierarchical tree structure corresponds to respective contents data reproducing device");

the processing device being operative to receive from the delegating device information representative of one or more of the nodes (pars 82, 84, 90-91, par 96 "provider delivers the ciphered common contents data or such a contents data key commonly usable by individual devices to those devices"),

the processing device being configured based on the received information for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality (pars 82, 84, 90-91);

wherein the nodes of the graph are arranged in a plurality of levels with one or more nodes at each level and wherein the nodes correspond to respective seeds (par 22 "these leaf-keys are respectively provided in correspondence with own leaves among a hierarchy key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of the key tree structure comprising a plurality of data processing apparatuses as own leaves");

wherein a first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level (pars 23-24, 97-105, 114-117);

the transmitted information including the first seed but not the second seed (par 96 "provider delivers the ciphered common contents data or such a contents data key commonly usable by individual devices to those devices").

As per **claim 30**, Okaue teaches a machine-readable storage medium containing one or more software programs for use in partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality from a delegating device to at least one recipient device, the cryptographic functionality being characterized as a graph comprising a plurality of nodes (par 15 "hierarchy key tree structure" ; par 16 "key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of the key tree structure comprising a plurality of devices"), wherein the one or more software programs when executed by the delegating device implement the steps of (par 30 "program providing medium is provided, which provides such a computer program to enable a computer system to execute"):

associating a given set of the nodes with a corresponding one of the plurality of distinct portions of the cryptographic functionality (par 22 "these leaf-keys are respectively provided in correspondence with own leaves among a hierarchy key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of the key tree structure comprising a plurality of data processing apparatuses as own leaves"; par 92 "each of individual leaves of the hierarchical tree structure corresponds to respective contents

data reproducing device"), and to transmit to the recipient device information representative of one or more of the nodes (pars 82, 84, 90-91, par 96 "provider delivers the ciphered common contents data or such a contents data key commonly usable by individual devices to those devices"); and

transmitting from the delegating device to the recipient device information representative of one or more of the nodes (pars 82, 84, 90-91, par 96 "provider delivers the ciphered common contents data or such a contents data key commonly usable by individual devices to those devices"),

the recipient device being configured based on the transmitted information for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality (pars 82, 84, 90-91);

wherein the nodes of the graph are arranged in a plurality of levels with one or more nodes at each level and wherein the nodes correspond to respective seeds (par 22 "these leaf-keys are respectively provided in correspondence with own leaves among a hierarchy key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of the key tree structure comprising a plurality of data processing apparatuses as own leaves");

wherein a first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level (pars 23-24, 97-105, 114-117);

the transmitted information including the first seed but not the second seed (par 96 "provider delivers the ciphered common contents data or such a contents data key commonly usable by individual devices to those devices").

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571) 272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Tamara Teslovich/
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437